IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

COALITION FOR INDEPENDENT TECHNOLOGY RESEARCH, *Plaintiff,*	§	
v.	§	No. 1:23-cv-00783
GREG ABBOTT, in his official capacity as Governor of the State of Texas, et al. STEVEN C. MCCRAW, in his official capacity as Director and Colonel of the Texas Department of Public Safety, AMANDA CRAWFORD, in her official capacity as Executive Director of the Texas Department of Information Resources and Chief Information Officer of Texas, DALE RICHARDSON, in his official capacity as Chief Operations Officer of the Texas Department of Information Resources, ASHOK MAGO, LAURA WRIGHT, LINDY RYDMAN, CARLOS MUNGUIA, MARY DENNY, MILTON B. LEE, MELISA DENIS, DANIEL FEEHAN, and JOHN SCOTT, JR., in their official capacities as members of the Board of Regents of the University of North Texas System, and MICHAEL WILLIAMS, in his official capacity as Chancellor of the University of North Texas System, *Defendants.*	§	

DECLARATION OF RICHARD ANDERSON

Richard Anderson declares:

1. I am the Associate Vice Chancellor and Chief Information Security Officer for the University of North Texas System ("UNT System"). UNT System is comprised of the University of

North Texas, the University of North Texas Health Science Center at Fort Worth, the University of North Texas at Dallas, and the University of North Texas System Administration.

2. I am responsible for overseeing and managing UNT System's information technology ("IT") security program, assessing and preventing cyberattacks or other unauthorized uses of UNT System's IT resources, and for numerous other information security areas for the entire UNT System. I have been employed within the UNT System in an IT security capacity since October 2001.

3. In addition, during my employment within the UNT System I have been an adjunct professor in the UNT Information Science Department and have taught graduate courses and seminars on cybersecurity, digital imaging, information theory, and other information science topics from 2014–2020. Currently, I advise graduate students working in the cybersecurity field. I have a PhD in Information Science and am a Certified Information Systems Security Professional and Certified Cloud Security Professional.

I. UNT System Implements the TikTok Ban.

4. UNT System banned TikTok on university-owned devices and networks, as directed by Governor Abbott's December 7, 2022 Executive Order. I was involved in UNT System's execution of the directive.

5. UNT System implemented the TikTok ban in two primary ways. First, UNT System blocked network traffic to and from TikTok. Second, UNT System scanned System-owned devices issued to employees (laptops and computers) using an endpoint security (colloquially referred to as "antivirus") tool to detect and remove the TikTok application on these devices.

6. UNT System scanned approximately 18,000 UNT System-owned computers and found that only six of them had the TikTok application installed. We removed the TikTok application on these six computers.

7. UNT System generally does not provide employees with cellphones, so these were not scanned during our efforts to detect and remove the TikTok application from UNT System-owned devices.

II. UNT System Comprehensively Regulates its IT Resources.

8. UNT System comprehensively regulates use of its IT resources, such as university-owned devices and networks. Many of the restrictions on UNT System's IT resources can be found in UNT System's 2022 Information Security Handbook, which is attached as **Exhibit 3**.

9. For instance, access to UNT System's files and networks are userID and password protected, meaning UNT System controls who is authorized to access these resources at all times.

10. UNT System provides devices, like laptops, to certain employees and provides individuals who are authorized to use UNT System's IT resources access to its networks. But UNT System owns these devices and networks. UNT System retains the right to revoke authorized users of its devices and networks access to the devices and networks, to remove or add applications on the devices, and to control use of the devices and networks in other ways. Also, an employee must return a provided device when his or her employment with UNT System terminates.

III. UNT System is Subjected to Constant Cyberattacks, Sometimes from Foreign Governments.

11. Hackers present a serious and constant threat to UNT System's security. For instance, there are 12,049 phishing attacks on average against UNT System each day. Examples of phishing attacks against UNT System include financial scams; attempts to get targeted users to give the attacker user names, passwords, multifactor credentials, or other types of sensitive information; and attempts to get targeted users to install malware, ransomware or remote access tools on the attackers' behalf.

12. Also, there are an average of 621 malware attacks that require either automated or manual incident response against UNT System per month during the calendar year of 2023. Examples

of malware attacks attempted against UNT System include ransomware, information stealing, cryptocurrency mining, remote control, and surveillance tools.

13. Further, there are an average of 75,753 network attacks against UNT System each day. Examples of network attacks against UNT System include vulnerability scans, SQL ("Structured Query Language") injection attacks against databases, and attacks against public-facing web servers.

14. These cyberattacks could seriously disrupt UNT System's operations or otherwise threaten the confidentiality, integrity, and availability of UNT System data or information systems if successful.

15. I have reasonable grounds for believing that foreign governments have sponsored some of the cyberattacks against UNT System.

IV. UNT System Could Not Reasonably Limit its TikTok Ban to Only Employees with Access to "Sensitive Information."

16. I have reviewed the Declaration of Bruce Schneier that Plaintiff filed during this case.[1] There, Schneier proposes that the concerns associated with TikTok "could be addressed with a much narrower policy" than what UNT System implemented, such as a policy that limits the ban to "university employees who have access to sensitive information."[2]

17. Schneier's proposal would be unworkable. The primary impediment is that nearly all UNT System employees, including faculty, have access to sensitive records protected by the Family Educational Rights and Privacy Act. This is unavoidable due to UNT System's status as an institution of higher education with the extensive scope of records protected by FERPA.

18. UNT System maintains other types of sensitive files, including financial aid and other financial documents, medical records, other records that are confidential by federal and state law, and proprietary data. Given the breadth of sensitive files maintained by UNT System and the number of

[1] ECF 20-3.
[2] *Id.* at ¶ 48.

employees with access to such files, it would be highly difficult, if not practically impossible, to limit a TikTok ban to only employees with access to sensitive information.

19. I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 12, 2023

Richard Anderson